CLAIMS

WHAT IS CLAIMED IS:

1. A device for use in a personal computer system, wherein the device comprises a storage location for storing a GUID, wherein the device is configured to provide the GUID to a master in the computer system during a trusted setup, and wherein the device is further configured to provide at least an indication of the GUID during a data transaction.

2. The device of claim 1 further configured to encrypt the indication of the GUID during the data transaction.

3. The device of claim 1 further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret during the data transaction.

4. The device of claim 3, wherein the secret comprises a system GUID.

5. The device of claim 3 configured to encrypt the data using only the secret and to transmit only the encrypted data.

6. The device of claim 5, further configured to encrypt the data using the secret and the GUID.

7. The device of claim 1 configured to receive a nonce or random number during a data transaction, wherein the device is further configured to provide at least the indication of the GUID during the data transaction using a hash of the GUID and the nonce or random number.

8. The device of claim 7 further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret during the data transaction.

9. The device of claim 8 further configured to encrypt the data using the GUID, the secret, and the nonce or random number.

10. The device of claim 7 further configured to respond to the data transaction in response to receiving the nonce or random number.

11. The device of claim 10 further configured to respond to the data transaction only in response to receiving the nonce or random number.

12. The device of claim 7 further configured to encrypt the data using the GUID and to transmit only the encrypted data and the nonce or random number.

13. The device of claim 12 further configured to encrypt the data using the GUID and the nonce or random number.

14. The device of claim 1, wherein the device is comprised in a computer subsystem.

15. The device of claim 14, wherein the device is a memory module, and the computer subsystem is a memory controller.

16. The device of claim 14, wherein the device is a storage device, and the computer subsystem is a storage controller.

17. The device of claim 1, wherein the master is one of the group consisting of a computer subsystem, a processor, a south bridge, a north bridge, a chip on a computer motherboard, and a daughter card in a slot on the computer motherboard.

18. A device for use in a personal computer system, wherein the device comprises one or more storage locations for storing one or more of the group consisting of a GUID, a secret, and a system GUID; wherein the device is configured to perform during a trusted setup at least one or more from the group consisting of providing the GUID to a master in the computer system, receiving and storing the secret, and receiving and storing the system GUID; and wherein the device is further configured to provide at least an indication of one or more of the group consisting of the GUID, the secret, and the system GUID during a data transaction.

19. The device of claim 18, wherein the indication comprises one of the group consisting of the GUID, the secret, the system GUID, and a result of a hash using one or more of the group consisting of the GUID, the secret, and the system GUID.

20. The device of claim 18, wherein data transferred during the data transaction is encrypted using one or more of the group consisting of the GUID, the secret, and the system GUID.

21. The device of claim 18, wherein the device is a computer subsystem.

22. The device of claim 21, wherein the device is a memory module, and the computer subsystem is a memory controller.

23. The device of claim 21, wherein the device is a storage device, and the computer subsystem is a storage controller.

24. The device of claim 18, wherein the master is one of the group consisting of a computer subsystem, a processor, a south bridge, a north bridge, a chip on a computer motherboard, and a daughter card in a slot on the computer motherboard.

25. A computer system, comprising:

a master device; and

a device comprising a storage location for storing a GUID, wherein the device is configured to provide the GUID to the master device during a trusted setup, and wherein the device is further configured to provide at least an indication of the GUID during a data transaction.

26. The computer system of claim 25, wherein the device is further configured to encrypt the indication of the GUID during the data transaction.

27. The computer system of claim 25, wherein the device is further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret during the data transaction.

28. The computer system of claim 27, wherein the secret comprises a system GUID, wherein the system GUID is provided to the device during the trusted setup.

29. The computer system of claim 25, wherein the device is further configured to receive a nonce from the master device and to transmit the nonce during the data transaction.

30. The computer system of claim 29, wherein the device is further configured to encrypt the data using the nonce and to transmit only the encrypted data and the nonce during the data transaction; and wherein the master device is further configured to receive the encrypted data and the nonce from the device and to decrypt the encrypted data using the nonce.

31. The computer system of claim 29, wherein the device is further configured to receive a secret, to store the secret, and to transmit at least an indication of the secret with the data; and wherein the master device is further configured to receive at least the indication of the secret from the device and to authenticate the data as being from the device using at least the indication of the secret.

32. The computer system of claim 31, wherein the device is configured to encrypt the data using only the secret and to transmit only the encrypted data and the nonce.

33. The computer system of claim 31, wherein the device is further configured to encrypt the data for the data transaction using the GUID, the secret, and the nonce.

34. The computer system of claim 29, wherein the device is further configured to respond to the data transaction in response to receiving the nonce.

35. The computer system of claim 34, wherein he device is further configured to respond to the data transaction only in response to receiving the nonce.

36. The computer system of claim 29, wherein the nonce further comprises a random number.

37. The computer system of claim 25, wherein the device is a computer subsystem.

38. The computer system of claim 37, wherein the device is a memory module, and the master device is a memory controller.

39. The computer system of claim 37, wherein the device is a storage device, and the master device is a storage controller.

40. The computer system of claim 25, wherein the master device is one of the group consisting of a computer subsystem, a processor, a south bridge, a north bridge, a chip on a computer motherboard, and a daughter card in a slot on the computer motherboard.

41. A computer system, comprising:

a master device; and

a device comprising one or more storage locations for storing one or more of the group consisting of a GUID, a secret, and a system GUID; wherein the device is configured to perform during a trusted setup at least one or more from the group consisting of providing the GUID to the master device in the computer system, receiving and storing the secret from the

master device, and receiving and storing the system GUID from the master device; and wherein the device is further configured to provide at least an indication of one or more of the group consisting of the GUID, the secret, and the system GUID during a data transaction with the master device.

42. The computer system of claim 41, wherein the indication comprises one of the group consisting of the GUID, the secret, the system GUID, and a result of a hash using one or more of the group consisting of the GUID, the secret, and the system GUID.

43. The computer system of claim 41, wherein data transferred during the data transaction with the master device is encrypted using one or more of the group consisting of the GUID, the secret, and the system GUID.

44. The computer system of claim 41, wherein the device is comprised in a computer subsystem.

45. The computer system of claim 44, wherein the device includes a memory module, and the master device includes a memory controller.

46. The computer system of claim 44, wherein the device includes a storage device, and the computer subsystem includes a storage controller.

47. The computer system of claim 41, wherein the master device includes one of the group consisting of a computer subsystem, a processor, a south bridge, a north bridge, a chip on a computer motherboard, and a daughter card in a slot on the computer motherboard.

48. A method, comprising:

providing a GUID;

receiving a request for a data transaction;

transmitting data in the data transaction and at least an indication of the GUID in the data transaction; and

authenticating the data using at least the indication of the GUID in the data transaction.

49. The method of claim 48, further comprising:

providing a nonce in the data transaction;

receiving the nonce in the data transaction;

wherein transmitting data in the data transaction and at least an indication of the GUID in the data transaction further comprises transmitting the nonce with the data and at least the indication of the GUID in the data transaction; and

wherein authenticating the data using at least the indication of the GUID in the data transaction further comprises authenticating the data using at least the indication of the GUID and the nonce in the data transaction.

50. The method of claim 49, further comprising:

encrypting the data using the GUID to form encrypted data;

wherein transmitting the nonce with the data and at least the indication of the GUID in the data transaction comprises transmitting only the encrypted data and the nonce;

receiving the encrypted data and the nonce; and

decrypting the encrypted data using the GUID.

51. The method of claim 49,

wherein encrypting the data using the GUID to form encrypted data further comprises encrypting the data using the GUID and the nonce; and

wherein decrypting the encrypted data using the GUID comprises decrypting the encrypted data using the GUID and the nonce.

52. The method of claim 49, further comprising:

receiving a secret;

storing the secret;

wherein transmitting the nonce with the data and at least the indication of the GUID in the data transaction further comprises transmitting at least an indication of the secret with the data;

receiving at least the indication of the secret with the data; and

wherein authenticating the data using at least the indication of the GUID and the nonce in the data transaction further comprises authenticating the data using at least the indication of the GUID, at least the indication of the secret, and the nonce in the data transaction.

53. The method of claim 52,

wherein encrypting the data using the GUID to form encrypted data further comprises encrypting the data using the GUID and the secret to form encrypted data; and

wherein decrypting the encrypted data using the GUID comprises decrypting the encrypted data using the GUID and the secret.

54. The method of claim 53,

wherein encrypting the data using the GUID and the secret to form encrypted data comprises encrypting the data using the GUID, the secret, and the nonce; and

wherein decrypting the encrypted data using the GUID and the secret further comprises decrypting the encrypted data using the GUID, the secret, and the nonce.

55. The method of claim 52, wherein the secret comprises a system GUID,

wherein receiving the secret comprises receiving the system GUID;

wherein storing the secret comprises storing the system GUID;

wherein transmitting at least the indication of the secret with the data comprises transmitting at least the indication of the system GUID with the data;

wherein receiving at least the indication of the secret with the data comprises receiving at least the indication of the system GUID with the data; and

wherein authenticating the data using at least the indication of the GUID, at least the indication of the secret, and the nonce in the data transaction comprises authenticating the data using at least the indication of the GUID, at least the indication of the system GUID, and the nonce in the data transaction.

56. The method of claim 49, wherein transmitting the data in the data transaction occurs in response to providing the nonce in the data transaction.

57. The method of claim 56, wherein transmitting the data in the data transaction occurs only in response to providing the nonce in the data transaction.

58. The method of claim 49, wherein the nonce comprises a random number;

wherein providing the nonce in the data transaction comprises providing the random number in the data transaction;

wherein receiving the nonce in the data transaction comprises receiving the random number in the data transaction; and

wherein further transmitting the nonce with the data and at least the indication of the GUID in the data transaction comprises transmitting the random number with the data and at least the indication of the GUID in the data transaction.

59. A method, comprising:

providing a GUID to a master device during a trusted setup;

setting an introduced bit during the trusted setup;

receiving a data transaction request; and

refusing the data transaction request once the introduced bit is set unless at least an indication of the GUID is provided in the data transaction request.

60. The method of claim 59, further comprising:

accepting the data transaction request once the introduced bit is set and at least an indication of the GUID is provided in the data transaction request.

61. The method of claim 59, further comprising:

receiving a system GUID from the master device; and

storing the system GUID.

62. The method of claim 61, further comprising:

requesting at least an indication of the system GUID in response to receiving the data transaction request; and

wherein refusing the data transaction request once the introduced bit is set unless at least the indication of the GUID is provided in the data transaction request further comprises refusing the data transaction request once the introduced bit is set unless at least the indication of the system GUID is provided.

63. The method of claim 62,

wherein accepting the data transaction request once the introduced bit is set and at least the indication of the GUID is provided in the data transaction request further comprises accepting the data transaction request once the introduced bit is set and at least the indication of the system GUID is provided.

64. The method of claim 59, further comprising:

receiving a request for the introduced bit to be reset from a requestor;

requesting at least an indication of the GUID or the system GUID from the requestor;

receiving at least the indication of the GUID or the system GUID from the requestor; and

resetting the introduced bit.

65. The method of claim 59, further comprising:

providing a key configured to reset the introduced bit;

receiving the key configured to reset the introduced bit;

authenticating the key configured to reset the introduced bit; and

resetting the introduced bit in response to authenticating the key configured to reset the introduced bit.

66. A computer system, comprising:

means for providing a GUID to a master device during a trusted setup;

means for setting an introduced bit during the trusted setup;

means for receiving a data transaction request; and

means for refusing the data transaction request once the introduced bit is set unless at least an indication of the GUID is provided in the data transaction request.

67. The computer system of claim 66, further comprising:

means for accepting the data transaction request once the introduced bit is set and at least an indication of the GUID is provided in the data transaction request.

68. The computer system of claim 66, further comprising:

means for receiving a system GUID from the master device; and

means for storing the system GUID.

69. A system, comprising:

a first device, including a timer and logic coupled to the timer; and

a security authenticator configured to authenticate the first device, wherein the security authenticator is further configured to provide at least an indication to the logic that the

timer is to be reset to a predetermined value in response to authenticating the first device.

70. The system of claim 69, further comprising:

a subsystem, wherein the security authenticator is comprised in the subsystem.

71. The system of claim 70, wherein the device includes a memory module and the subsystem includes a memory controller.

72. The system of claim 71, wherein the device includes a data storage device and the subsystem includes a data storage controller.

73. The system of claim 69, further comprising:

a network connection, wherein the security authenticator is coupled to the device through the network connection.

74. The system of claim 69, wherein the device includes a portable computer.

75. A computer system, comprising:

a first device, including a first timer and first logic coupled to the first timer;

a second device including a second timer and second logic coupled to the second timer, wherein the second device also includes a first security authenticator configured to authenticate the first device, wherein the first security authenticator is further configured to provide at least an indication to the first logic that the first timer is to be reset to a first predetermined value in response to authenticating the first device; and

a second security authenticator configured to authenticate the second device, wherein the second security authenticator is further configured to provide at least an indication to the second logic that the second timer is to be reset to a second predetermined value in response to authenticating the second device.

76. The computer system of claim 75, further comprising:

a subsystem, wherein the second device is comprised in the subsystem.

77. The computer system of claim 75, wherein the first device includes a memory module and the second device includes a memory controller.

78. The computer system of claim 75, wherein the first device includes a data storage device and the second device includes a data storage controller.

79. The computer system of claim 75, further comprising:

a network connection, wherein the second security authenticator is coupled to the second device through the network connection.

80. The computer system of claim 79, further comprising:

a server, wherein the server includes the second security authenticator.

81. The computer system of claim 75, wherein the second device includes a portable computer.

82. The computer system of claim 75, wherein the first device is comprised in a south bridge.

83. The computer system of claim 75, wherein the first device is comprised in a crypto-processor.

84. A method of operating a computer system, the method comprising:

authenticating a first device;

setting a starting value on a timer;

updating the timer in a predetermined manner; and

authenticating the first device if the timer has expired.

85. The method of claim 84, wherein the first device comprises a memory module; wherein authenticating the first device comprises authenticating the memory module; wherein setting the starting value on the timer comprises setting the starting value on the timer associated with the memory module; wherein updating the timer in the predetermined manner comprises updating the timer associated with the memory module in the predetermined manner; and wherein authenticating the first device if the timer has expired comprises authenticating the memory module if the timer associated with the memory module has expired.

86. The method of claim 84, wherein the first device comprises a data storage device; wherein authenticating the first device comprises authenticating the data storage device; wherein setting the starting value on the timer comprises setting the starting value on the timer associated with the data storage device; wherein updating the timer in the

predetermined manner comprises updating the timer associated with the data storage device in the predetermined manner; and wherein authenticating the first device if the timer has expired comprises authenticating the data storage device if the timer associated with the data storage device has expired.

87. The method of claim 84, wherein authenticating the first device comprises authenticating the first device over a network; and wherein authenticating the first device if the timer has expired comprises authenticating the first device over the network if the timer has expired.

88. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

computer readable program storage device, comprising:

providing a GUID;

receiving a request for a data transaction;

transmitting data in the data transaction and at least an indication of the GUID in the data transaction; and

authenticating the data using at least the indication of the GUID in the data transaction.

89. The computer readable program storage device of claim 88, the method further comprising:

providing a nonce in the data transaction;

receiving the nonce in the data transaction;

wherein transmitting data in the data transaction and at least an indication of the GUID in the data transaction further comprises transmitting the nonce with the data and at least the indication of the GUID in the data transaction; and

wherein authenticating the data using at least the indication of the GUID in the data transaction further comprises authenticating the data using at least the indication of the GUID and the nonce in the data transaction.

90. The computer readable program storage device of claim 89, the method further comprising:

encrypting the data using the GUID to form encrypted data;

wherein transmitting the nonce with the data and at least the indication of the GUID in the data transaction comprises transmitting only the encrypted data and the nonce;

receiving the encrypted data and the nonce; and

decrypting the encrypted data using the GUID.

91. The computer readable program storage device of claim 89,

wherein encrypting the data using the GUID to form encrypted data further comprises encrypting the data using the GUID and the nonce; and

wherein decrypting the encrypted data using the GUID comprises decrypting the encrypted data using the GUID and the nonce.

92. The computer readable program storage device of claim 89, the method further comprising:

receiving a secret;

storing the secret;

wherein transmitting the nonce with the data and at least the indication of the GUID in the data transaction further comprises transmitting at least an indication of the secret with the data;

receiving at least the indication of the secret with the data; and

wherein authenticating the data using at least the indication of the GUID and the nonce in the data transaction further comprises authenticating the data using at least the indication of the GUID, at least the indication of the secret, and the nonce in the data transaction.

93. The computer readable program storage device of claim 92,

wherein encrypting the data using the GUID to form encrypted data further comprises encrypting the data using the GUID and the secret to form encrypted data; and

wherein decrypting the encrypted data using the GUID comprises decrypting the encrypted data using the GUID and the secret.

94. The computer readable program storage device of claim 93,

wherein encrypting the data using the GUID and the secret to form encrypted data comprises encrypting the data using the GUID, the secret, and the nonce; and

wherein decrypting the encrypted data using the GUID and the secret further comprises decrypting the encrypted data using the GUID, the secret, and the nonce.

95. The computer readable program storage device of claim 92, wherein the secret comprises a system GUID,

wherein receiving the secret comprises receiving the system GUID;

wherein storing the secret comprises storing the system GUID;

wherein transmitting at least the indication of the secret with the data comprises transmitting at least the indication of the system GUID with the data;

wherein receiving at least the indication of the secret with the data comprises receiving at least the indication of the system GUID with the data; and

wherein authenticating the data using at least the indication of the GUID, at least the indication of the secret, and the nonce in the data transaction comprises authenticating the data using at least the indication of the GUID, at least the indication of the system GUID, and the nonce in the data transaction.

96. The computer readable program storage device of claim 89, wherein transmitting the data in the data transaction occurs in response to providing the nonce in the data transaction.

97. The computer readable program storage device of claim 96, wherein transmitting the data in the data transaction occurs only in response to providing the nonce in the data transaction.

98. The computer readable program storage device of claim 89, wherein the nonce comprises a random number;

wherein providing the nonce in the data transaction comprises providing the random number in the data transaction;

wherein receiving the nonce in the data transaction comprises receiving the random number in the data transaction; and

wherein further transmitting the nonce with the data and at least the indication of the GUID in the data transaction comprises transmitting the random number with the data and at least the indication of the GUID in the data transaction.

99. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

providing a GUID to a master device during a trusted setup;

setting an introduced bit during the trusted setup;

receiving a data transaction request; and

refusing the data transaction request once the introduced bit is set unless at least an indication of the GUID is provided in the data transaction request.

100. The computer readable program storage device of claim 99, the method further comprising:

accepting the data transaction request once the introduced bit is set and at least an indication of the GUID is provided in the data transaction request.

101. The computer readable program storage device of claim 99, the method further comprising:

receiving a system GUID from the master device; and

storing the system GUID.

102. The computer readable program storage device of claim 101, the method further comprising:

requesting at least an indication of the system GUID in response to receiving the data transaction request; and

wherein refusing the data transaction request once the introduced bit is set unless at least the indication of the GUID is provided in the data transaction request further comprises refusing the data transaction request once the introduced bit is set unless at least the indication of the system GUID is provided.

103. The computer readable program storage device of claim 102,

wherein accepting the data transaction request once the introduced bit is set and at least the indication of the GUID is provided in the data transaction request further comprises accepting the data transaction request once the introduced bit is set and at least the indication of the system GUID is provided.

104. The computer readable program storage device of claim 99, the method further comprising:

receiving a request for the introduced bit to be reset from a requestor;

requesting at least an indication of the GUID or the system GUID from the requestor;

receiving at least the indication of the GUID or the system GUID from the requestor; and

resetting the introduced bit.

105. The computer readable program storage device of claim 99, the method further comprising:

providing a key configured to reset the introduced bit;

receiving the key configured to reset the introduced bit;

authenticating the key configured to reset the introduced bit; and

resetting the introduced bit in response to authenticating the key configured to reset the introduced bit.

106. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of operating the computer system, the method comprising:

authenticating a first device;

setting a starting value on a timer;

updating the timer in a predetermined manner; and

authenticating the first device if the timer has expired.

107. The computer readable program storage device of claim 106, wherein the first device comprises a memory module; wherein authenticating the first device comprises authenticating the memory module; wherein setting the starting value on the timer comprises setting the starting value on the timer associated with the memory module; wherein updating the timer in the predetermined manner comprises updating the timer associated with the memory module in the predetermined manner; and wherein authenticating the first device if the timer has expired comprises authenticating the memory module if the timer associated with the memory module has expired.

108. The computer readable program storage device of claim 106, wherein the first device comprises a data storage device; wherein authenticating the first device comprises authenticating the data storage device; wherein setting the starting value on the timer comprises setting the starting value on the timer associated with the data storage device; wherein updating the timer in the predetermined manner comprises updating the timer

associated with the data storage device in the predetermined manner; and wherein authenticating the first device if the timer has expired comprises authenticating the data storage device if the timer associated with the data storage device has expired.

109. The computer readable program storage device of claim 106, wherein authenticating the first device comprises authenticating the first device over a network; and wherein authenticating the first device if the timer has expired comprises authenticating the first device over the network if the timer has expired.